BOK FINANCIAL

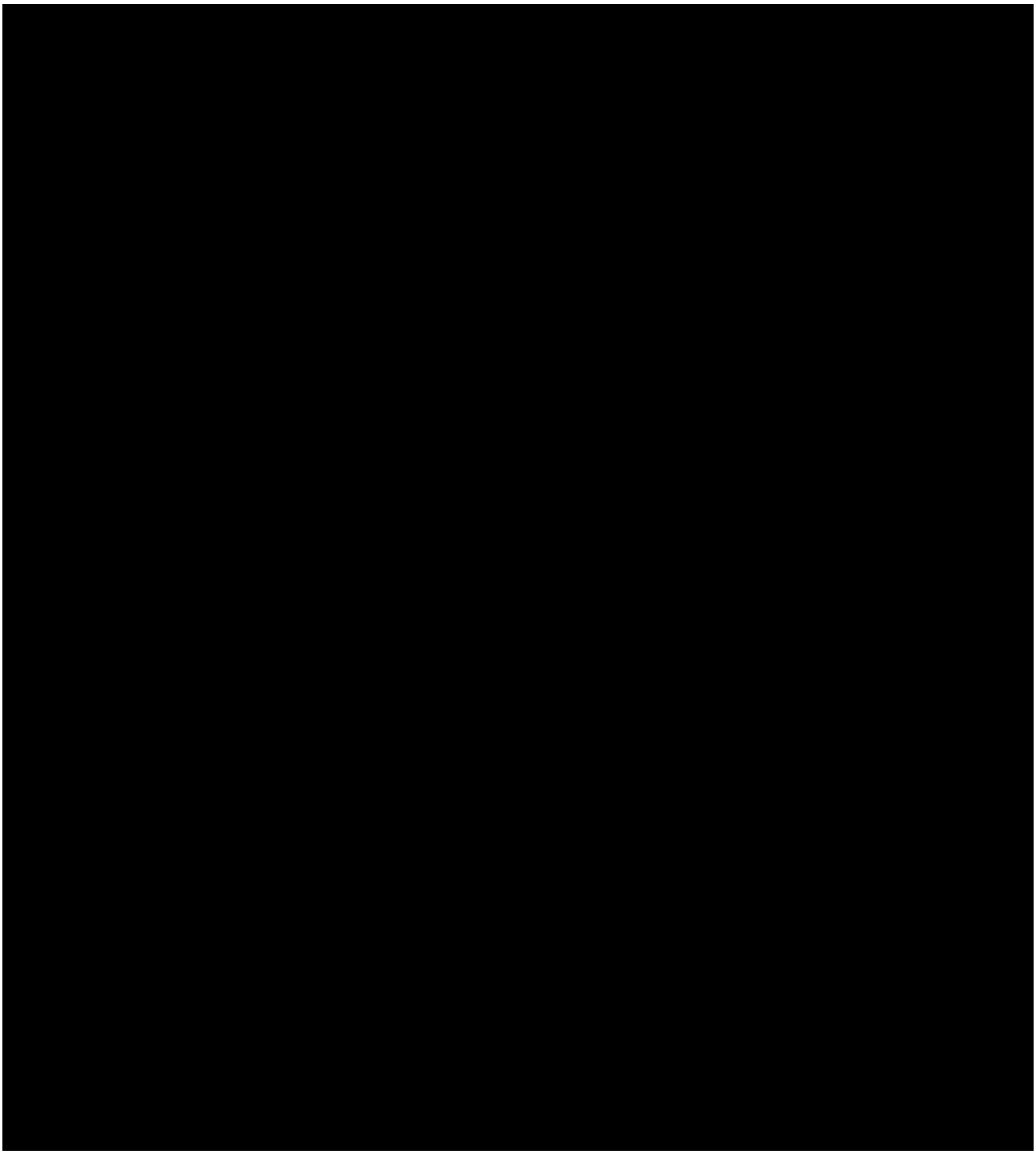
Policy ID #:X2701.07

Standards of Conduct

This policy is applicable to BOK Financial Corporation, BOKF, NA and its divisions, affiliates and subsidiaries

DOCUMENT CONTROL

Managed by: Teil Blackshare	**Responsible position:** Director, Operational Risk
Contact person: Kelly Reed	**Approved by:** Audit Committee of the Board of Directors
Contact position: Manager, Risk Assessment & Governance	**Date approved:** 5/2/2023
Contact number: 918-921-3036	**Next review date:** Annual



3.4.6.3 INFORMATION, SYSTEMS, AND DATA SECURITY

3.4.6.3.1 Company Assets

Systems used to store, record, process, and access information, and Company data are Company assets. The loss, destruction, or unauthorized disclosure of information, or of components of information, can cause irreparable damage to the Company and its customers. Use of Company provided internet, intranet, email, and digital media is limited to employees and authorized individuals for business purposes and is subject to monitoring by the Company.

3.4.6.3.2 Passwords and Access Codes.

Passwords and access codes, including security badges, are the personal responsibility of each employee, must be protected, and may not be shared.

3.4.6.3.3 Record Retention.

Records must be retained in accordance with applicable laws, regulations, and Company policies, practices, and procedures.

Computer and other electronic files should be disposed of in accordance with the Information Security Program Policy (ISPP), Email Retention Policy, and Company policies.

3.4.6.3.4 Protection of Data.

Company employees must protect sensitive customer, vendor, and/or Company information (data) at all times and in accordance with the Information Security Program Policy (ISPP), ISPP Asset Handling Policy, and departmental policies and practices. See, in particular, Information Security Program Policy, ISPP Asset Handling Policy, and Termination/Separation Policy. See also: respective line of business policies, procedures, practices, and/or agreements, including, but not limited to, Work from Home Agreements and BOK Financial Securities, Inc. Representative Agreements. Electronic data and Hard Copy data shall not be maintained in a vehicle or otherwise unsecured.

3.4.6.3.4.1 Electronic Data.

Subject to Section 3.2, and adequate precautions to protect data disclosed pursuant to Section 3.2, confidential information and/or Company information should be maintained only on Company secure systems. Specifically, employees are reminded that use of personal email accounts, social media (unless a limited exception is approved by the Company for marketing purposes), instant messaging services, or other forms of electronic communications and/or data storage, to conduct business outside BOKF data security controls is prohibited. See also: Social Media Policy.

3.4.6.3.4.2 Hard Copy Data.

Subject to Section 3.2, and adequate precautions to protect data disclosed pursuant to Section 3.2, confidential and/or proprietary information that is maintained in hard copy, must be accessed and handled for business necessity only, should only be used when it is impractical to use electronic access, and must be maintained as confidential and handled pursuant to the most restrictive respective line of business policies, procedures, practices, and/or agreements, including, but not limited to, Work From Home Agreements and BOK Financial Securities, Inc. Representative Agreements.

3.4.6.4 RESPONSIBILITIES.

It is the employee's and the supervisor's responsibility to ensure that no employee, contractor, vendor, or non-employee, has access to systems and/or data not necessary for that person's assigned work functions on behalf of the Company.

It is the responsibility of the individual employee terminating employment and the immediate supervisor to see that confidential information and/or means of access to such information is, as soon a reasonably practicable, and if possible in advance of the terminating event, removed from

any employee who should terminate employment from the Company, by contacting the Employee Resource Center at 1-800-2My-BOKF (855.269.2653). See: Termination/Separation Policy.

3.4.6.5 CONFIDENTIAL PROPERTY AND INFORMATION

Employees are responsible for maintaining confidentiality of confidential materials or Company information, such as:

- Policies and procedures and practice manuals and guidance
- Account information
- Customer Contact Information
- Technical knowledge
- Marketing material
- Information technology
- Information that could supply the Company's competitors with a "competitive advantage"
- Information kept on a confidential basis, e.g. committee material and minutes
- Information not given or otherwise communicated to any other institution for their use

3.4.6.6 PROHIBITED USE OF BOKF PROPERTY

Company funds, property, services, supplies, facilities, or other things of value must not be used directly or indirectly by any employee of the Company to compensate any other bank, competitor, person, or entity for services, property, or loans made directly or indirectly to the employee, or for the benefit of the employee's family.

3.4.6.7 SAMPLE QUESTIONS & ANSWERS:

Q: When I work from home, I bring customer information with me and use my personal email address to send electronic files to my home computer. Am I allowed to do this?

A: Company work should be performed on a Company laptop or through a company approved VPN or other secured and authorized solution, and must follow Companysecurity measures.

Q: My friend who works for a company that does not compete with our company asked for the names of my business contacts. Am I allowed to give him this information?

A: No. Company employee, vendor, and/or client information is confidential. Employees may not share confidential data outside of the Reporting Methods in Section 4.

3.4.6.8 RECORDING OF TELEPHONE CONVERSATIONS, COMPANY VIDEO SECURITY, AND LACK OF PRIVACY OF INFORMATION ON COMPANY SYSTEMS.

Lack of Privacy. Many Company employees, whether as employees and/or as employees who are also customers of the Company, will have their conversations and/or activities recorded on Company systems. The conversations and/or activities may be maintained by the Company and may be accessed by the employee's supervisor, the compliance department, the audit department, senior management, law enforcement agencies, and regulatory bodies with oversight over Company entities. Conversations, communications, other writings, and activities on audio and/or video recordings may be utilized for business purposes, by senior management at senior management's business discretion including use in responses to law enforcement agencies, regulatory bodies with oversight over the Company, arbitration, and/or litigation.

Employees have no expectation of privacy with respect to recorded conversations and/or communications and/or activities recorded on and/or maintained on Company systems.

Limitations on Personal Use and Reasons For Limitations. The foregoing notwithstanding, use of employee personal audio and/or video recording devices or audio recording devices and personal use of Company recording devices risks violation of customer confidentiality, employee and company security, and employee privacy. For the foregoing reasons, use of employee personal audio and/or video recording devices or audio recording devices and personal use of Company recording devices, which might risk customer confidentiality, employee and company security and employee privacy, is prohibited without the express written prior permission of senior management and/or Human Resources. General Employees considering personal recording of a Company matter and/or person, must contact Human Resources and/or utilize the Reporting mechanisms in Section 4 REPORTING and Section 5 REQUESTS FOR EXCEPTIONS, INTERPRETATIONS AND DISPOSITION. *See also:* Section 3.3 NLRA.

Acknowledgement. By acknowledging these Standards of Conduct, the employee is specifically acknowledging both: (i) the lack of privacy of telephone conversations, communications, and other writings and/or audio and/or video stored on Company systems and (ii) limitations on personal use of audio/recording devices for the protection of customer confidentiality, employee and Company security, and employee privacy.

Item ID	Item Type	Revision Date	Revision Number	Title	User ID	Last Name	First Name	Middle Name	Completion Status ID	Completion Status	Completion Date
HR_SOC_2016	COURSE	2/5/2016 10:06 AM America/New York	1	Standards of Conduct 2016	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	4/25/2016 03:39 PM America/New York
BOKF_RM_SOC2019_EMPL_19	COURSE	5/30/2019 09:36 AM America/New York	1	Standards of Conduct 2019 Attestation	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	6/25/2019 05:41 PM America/New York
BOKF_RM_SOC2019_EMPL_19	COURSE	5/30/2019 09:36 AM America/New York	1	Standards of Conduct 2019 Attestation	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	7/8/2019 09:54 AM America/New York
BOKF_RM_SOC_EMPL_20	COURSE	5/20/2020 03:19 PM America/New York	1	Standards of Conduct 2020 Attestation	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	6/1/2020 10:45 AM America/New York
BOKF_RM_SOC_EMPL_21	COURSE	5/19/2021 09:36 AM America/New York	1	Standards of Conduct 2021 Attestation	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	6/27/2021 02:20 PM America/New York
BOKF_RM_SOC_EMPL_22v1	COURSE	5/26/2022 12:00 PM America/New York	1	Standards of Conduct 2022 Attestation	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	6/2/2022 12:51 PM America/New York
BOKF_RM_SOC_EMPL_23v2	COURSE	6/27/2023 08:15 PM America/New York	1	Standards of Conduct 2023 Attestation	*********	Bowen	Kyle	R	COURSE-COMPLETE	Course Complete	7/25/2023 10:42 AM America/New York